



*Up-to-date Questions and Answers from authentic resources to improve knowledge and pass the exam at very first attempt. ---- Guaranteed.*



SPLK-1003 MCQs  
SPLK-1003 TestPrep  
SPLK-1003 Study Guide  
SPLK-1003 Practice Test  
SPLK-1003 Exam Questions



**Splunk**

# SPLK-1003

*Splunk Enterprise Certified Admin*



**Question: 147**

Within props.conf, which stanzas are valid for data modification? (Choose all that apply.)

- A. Host
- B. Server
- C. Source
- D. Sourcetype

**Answer: CD**

Explanation:

Reference: <https://answers.splunk.com/answers/3687/host-stanza-in-props-conf-not-being-honored-forudp-514-data-sources.html>

**Question: 148**

Within props.conf, which stanzas are valid for data modification? (Choose all that apply.)

- A. Host
- B. Server
- C. Source
- D. Sourcetype

**Answer: CD**

Explanation:

Reference: <https://answers.splunk.com/answers/3687/host-stanza-in-props-conf-not-being-honored-forudp-514-data-sources.html>

**Question: 149**

Within props.conf, which stanzas are valid for data modification? (Choose all that apply.)

- A. Host
- B. Server
- C. Source
- D. Sourcetype

**Answer: CD**

Explanation:

Reference: <https://answers.splunk.com/answers/3687/host-stanza-in-props-conf-not-being-honored-forudp-514-data-sources.html>

**Question: 150**

This file has been manually created on a universal forwarder:

```
/opt/splunkforwarder/etc/apps/my_TA/local/inputs.conf
```

```
[monitor:///var/log/messages]
```

sourcetype=syslog

index=syslog

A new Splunk admin comes in and connects the universal forwarders to a deployment server and deploys the same app with a new inputs.conf file:

```
/opt/splunk/etc/deployment-apps/my_TA/local/inputs.conf
```

```
[monitor:///var/log/maillog]
```

sourcetype=maillog

index=syslog

Which file is now monitored?

- A. /var/log/messages
- B. /var/log/maillog
- C. /var/log/maillog and /var/log/messages
- D. none of the above

**Answer: A**

Explanation:

Reference: <https://docs.splunk.com/Documentation/Splunk/7.3.1/Updating/Exampleaddaninputtoforwarders>

**Question: 151**

Which forwarder type can parse data prior to forwarding?

- A. Universal forwarder
- B. Heaviest forwarder
- C. Hyper forwarder
- D. Heavy forwarder

**Answer: D**

Explanation:

Reference: <https://docs.splunk.com/Documentation/Splunk/7.3.1/Forwarding/Typesofforwarders>

**Question: 152**

In which Splunk configuration is the SEDCMD used?

- A. props.conf
- B. inputs.conf
- C. indexes.conf
- D. transforms.conf

**Answer: A**

Explanation:

Reference: <https://answers.splunk.com/answers/212128/why-sedcmd-configured-in-propsconf-is-workingduri.html>

**Question: 153**

In which phase of the index time process does the license metering occur?

- A. Input phase
- B. Parsing phase

- C. Indexing phase
- D. Licensing phase

**Answer: C**

Explanation:

Reference: <https://docs.splunk.com/Documentation/Splunk/7.3.1/Admin/HowSplunklicensingworks>

**Question: 154**

When running the command shown below, what is the default path in which deploymentserver.conf is created? splunk set deploy-poll deployServer:port

- A. SPLUNK\_HOME/etc/deployment
- B. SPLUNK\_HOME/etc/system/local
- C. SPLUNK\_HOME/etc/system/default
- D. SPLUNK\_HOME/etc/apps/deployment

**Answer: B**

Explanation:

Reference: <https://docs.splunk.com/Documentation/Splunk/7.3.1/Updating/Configureddeploymentclients>

**Question: 155**

In case of a conflict between a whitelist and a blacklist input setting, which one is used?

- A. Blacklist
- B. Whitelist
- C. They cancel each other out.
- D. Whichever is entered into the configuration first.

**Answer: A**

Explanation:

Reference: [https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=8&ved=2ahUKEwj0r6Lso6bkAhUqxYUKHbWIDz4QFjAHegQIAxAC&url=http%3A%2F%2Fsplunk.training%2Fshowpdf.asp%3Fdata%3D789BB6B10C1B4376B548D711B4377F3F4B511B437805A8EC11B437742EA8F11B43779B6FA211B4377E2407E11B43730AF97411B4377F3F4B511B437742EA8F11B43779B6FA211B43771F822111B437731365811B43746D0DC011B4377549EC611B4377BED81011B437789BB6B11B4376D8B14511B437731365811B4376B548D711B4377F3F4B511B4376FC19B311B43732E61E211B4377F3F4B511B437742EA8F11B43779B6FA211B43771F822111B437731365811B43746D0DC011B4377549EC611B4377BED81011B437789BB6B11B4376D8B14511B437731365811B4376B548D711B4377F3F4B511B4376FC19B311B43732E61E211B4376D8B14511B4377AD23D911B437789BB6B11B43730AF97411B4373989B2C11B437386E6F511B437386E6F511B4373DF6C0811B43737532BE11B4373BC039A11B437351CA5011B43737532BE11B43730AF97411B4375BD6DD511B43730AF97411B437564E8C211B43730AF97411B437%257C2318D1%257C11649A&usg=AOvVaw2e9sJweivuCkqTb4-Y9uW](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=8&ved=2ahUKEwj0r6Lso6bkAhUqxYUKHbWIDz4QFjAHegQIAxAC&url=http%3A%2F%2Fsplunk.training%2Fshowpdf.asp%3Fdata%3D789BB6B10C1B4376B548D711B4377F3F4B511B437805A8EC11B437742EA8F11B43779B6FA211B4377E2407E11B43730AF97411B4377F3F4B511B437742EA8F11B43779B6FA211B43771F822111B437731365811B43746D0DC011B4377549EC611B4377BED81011B437789BB6B11B4376D8B14511B437731365811B4376B548D711B4377F3F4B511B437742EA8F11B43779B6FA211B43771F822111B437731365811B43746D0DC011B4377549EC611B4377BED81011B437789BB6B11B4376D8B14511B437731365811B4376B548D711B4377F3F4B511B4376FC19B311B43732E61E211B4377F3F4B511B437742EA8F11B43779B6FA211B43771F822111B437731365811B43746D0DC011B4377549EC611B4377BED81011B437789BB6B11B4376D8B14511B437731365811B4376B548D711B4377F3F4B511B4376FC19B311B43732E61E211B4376D8B14511B4377AD23D911B437789BB6B11B43730AF97411B4373989B2C11B437386E6F511B437386E6F511B4373DF6C0811B43737532BE11B4373BC039A11B437351CA5011B43737532BE11B43730AF97411B4375BD6DD511B43730AF97411B437564E8C211B43730AF97411B437%257C2318D1%257C11649A&usg=AOvVaw2e9sJweivuCkqTb4-Y9uW)

**Question: 156**

The priority of layered Splunk configuration files depends on the file's:

- A. Owner
- B. Weight
- C. Context
- D. Creation time

**Answer: C**

Explanation:

Reference: <https://docs.splunk.com/Documentation/Splunk/7.3.0/Admin/Wheretofindtheconfigurationfiles>

**Question: 157**

Which of the following are supported configuration methods to add inputs on a forwarder? (Select all that apply.)

- A. CLI
- B. Edit inputs.conf
- C. Edit forwarder.conf
- D. Forwarder Management

**Answer:** AB

Explanation:

Reference:

[https://docs.splunk.com/Documentation/Forwarder/7.3.1/Forwarder/HowtoforwarddatatoSplunkEnterprise#Define\\_inputs\\_on\\_the\\_universal\\_forwarder\\_with\\_configuration\\_files](https://docs.splunk.com/Documentation/Forwarder/7.3.1/Forwarder/HowtoforwarddatatoSplunkEnterprise#Define_inputs_on_the_universal_forwarder_with_configuration_files)

**Question:** 158

Which parent directory contains the configuration files in Splunk?

- A. \$SPLUNK\_HOME/etc
- B. \$SPLUNK\_HOME/var
- C. \$SPLUNK\_HOME/conf
- D. \$SPLUNK\_HOME/default

**Answer:** A

Explanation:

Reference: <https://docs.splunk.com/Documentation/Splunk/7.3.1/Admin/Configurationfiledirectories>

**Question:** 159

Where should apps be located on the deployment server that the clients pull from?

- A. \$SPLUNK\_HOME/etc/apps
- B. \$SPLUNK\_HOME/etc/search
- C. \$SPLUNK\_HOME/etc/master-apps
- D. \$SPLUNK\_HOME/etc/deployment-apps

**Answer:** A

Explanation:

Reference: <https://answers.splunk.com/answers/371099/how-to-configure-deployment-apps-to-push-toclient.html>

**Question:** 160

Which Splunk component consolidates the individual results and prepares reports in a distributed environment?

- A. Indexers
- B. Forwarder
- C. Search head
- D. Search peers

**Answer:** A

Explanation:

Reference: <https://docs.splunk.com/Documentation/Splunk/7.3.1/Indexer/Advancedindexingstrategy>

**Question:** 161

Which Splunk component distributes apps and certain other configuration updates to search head cluster members?

- A. Deployer
- B. Cluster master
- C. Deployment server
- D. Search head cluster master

**Answer:** A

Explanation:

Reference: <https://docs.splunk.com/Documentation/Splunk/7.3.1/DistSearch/PropagateSHCconfigurationchanges>

**Question:** 162

You update a props.conf file while Splunk is running. You do not restart Splunk and you run this command: splunk btool props list C-debug.

What will the output be?

- A. A list of all the configurations on-disk that Splunk contains.
- B. A verbose list of all configurations as they were when splunkd started.
- C. A list of props.conf configurations as they are on-disk along with a file path from which the configuration is located.
- D. A list of the current running props.conf configurations along with a file path from which the configuration was made.

**Answer:** D

Explanation:

Reference: <https://answers.splunk.com/answers/494219/need-help-with-what-should-be-a-simpleprecedence.html>

**Question:** 163

Which setting in indexes.conf allows data retention to be controlled by time?

- A. maxDaysToKeep
- B. moveToFrozenAfter
- C. maxDataRetentionTime
- D. frozenTimePeriodInSecs

**Answer:** D

Explanation:

Reference: <https://docs.splunk.com/Documentation/Splunk/7.3.1/Indexer/SmartStoredataretention>

**Question:** 164

The universal forwarder has which capabilities when sending data? (Select all that apply.)

- A. Sending alerts
- B. Compressing data
- C. Obfuscating/hiding data
- D. Indexer acknowledgement

**Answer:** D

Explanation:

Reference: <https://docs.splunk.com/Documentation/Splunk/7.3.1/Forwarding/Typesofforwarders>

Killexams.com is a leading online platform specializing in high-quality certification exam preparation. Offering a robust suite of tools, including MCQs, practice tests, and advanced test engines, Killexams.com empowers candidates to excel in their certification exams. Discover the key features that make Killexams.com the go-to choice for exam success.



## Exam Questions:

Killexams.com provides exam questions that are experienced in test centers. These questions are updated regularly to ensure they are up-to-date and relevant to the latest exam syllabus. By studying these questions, candidates can familiarize themselves with the content and format of the real exam.

## Exam MCQs:

Killexams.com offers exam MCQs in PDF format. These questions contain a comprehensive collection of questions and answers that cover the exam topics. By using these MCQs, candidate can enhance their knowledge and improve their chances of success in the certification exam.

## Practice Test:

Killexams.com provides practice test through their desktop test engine and online test engine. These practice tests simulate the real exam environment and help candidates assess their readiness for the actual exam. The practice test cover a wide range of questions and enable candidates to identify their strengths and weaknesses.

## Guaranteed Success:

Killexams.com offers a success guarantee with the exam MCQs. Killexams claim that by using this materials, candidates will pass their exams on the first attempt or they will get refund for the purchase price. This guarantee provides assurance and confidence to individuals preparing for certification exam.

## Updated Contents:

Killexams.com regularly updates its question bank of MCQs to ensure that they are current and reflect the latest changes in the exam syllabus. This helps candidates stay up-to-date with the exam content and increases their chances of success.